UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

34415 7590 07/07/2006

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
LOVING, JARIC E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/612,198	NACHENBERG ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/17/03,8/30/04*. 100305
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear, in line 1, what "one command" refers to whether it is "commands that are accessing," from claim 1, line 4, or "acceptable commands," from claim 1, line 7.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 8-17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Desai et al., US 2003/0188189 and further in view of Harkins, US 6,775,827.

In claims 1 and 16, Desai discloses a computer implemented method and computer-readable medium containing computer program instructions for training a computer code intrusion detection system in real time (paragraphs [0035], [0043]), but fails to disclose: observing, in real time, commands that are accessing the computer code; and deriving from said commands, in real time, a set of acceptable commands.

Harkins discloses observing, in real time, commands that are accessing the computer code (col. 4, lines 13-17); and deriving from said commands, in real time, a set of acceptable commands (col. 5, lines 41-49 – execution profiles contain frequently selected commands, thus they are similar to set of acceptable commands).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system with Harkins' real time audit method that observe and derive acceptable commands to effectively examine programs during execution in real time. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system with real time auditing because it provides a quick, comprehensive analysis of a program's execution and also allows identification and resolution of any problems (Harkins, col. 2, lines 10-23).

In claim 2, Desai, as modified, discloses the method of claim 1 wherein the computer code is a database, and the computer code intrusion detection system is a dataase intrusion detection system (Desai, paragraphs [0052], [0056]).

In claim 3, Desai, as modified, discloses the method of claim 2 wherein the commands are SQL commands (Desai, paragraph [0056]).

In claim 4, Desai, as modified, discloses the method of claim 1 wherein at least one command is from the group of commands comprising a query, an add, a delete, and a modify (Desai, paragraphs [0052], [0092] – search of a database is similar to query).

In claims 5 and 17, Desai, as modified, discloses the method and computer-readable medium of claims 1 and 16, respectively, wherein the deriving step comprises:

grouping the commands into categories (Desai, paragraphs [0050]-[0052]); and

updating statistical information pertaining to the categories in real time (Desai, paragraph [0062]).

In claim 6, Desai, as modified, discloses the method of claim 5 wherein the categories comprise at least one category from the group of categories comprising:

canonicalized commands;

dates and times at which commands access the computer code (Desai, paragraphs [0050]-[0052]);

logins of users that issue commands;

identities of users that issue commands;

departments of users that issue commands;

applications that issue commands;

IP addresses of issuing users;

frequency of issuing commands by users;

identities of users accessing a given field within the computer code;

times of day that a given user accesses a given field within the computer code;

fields accessed by commands;

combinations of fields accessed by commands;

tables within the computer code accessed by commands;

combinations of tables within the computer code accessed by commands.

In claim 8, Desai, as modified, discloses the method of claim 1 wherein the observing step comprises at least one of:

real-time auditing (Harkins, col. 4, lines 13-17); and

in-line interception (Desai, paragraph [0042]).

In claim 9, Desai, as modified, discloses the method of claim 8 wherein the observing step comprises real-time auditing; and at least one of the following is used to extract the commands for observation:

an API that accesses the computer code;

code injection (col. 9, lines 5-28);

patching;

direct database integration.

In claim 10, Desai, as modified, discloses the method of claim 8 wherein the observing step comprises in-line interception; and at least one of the following is interposed between senders of the commands and the computer code:

a proxy;

a firewall (Desai, paragraph [0042]);

a sniffer (Desai, paragraph [0091]);

In claim 11, Desai, as modified, discloses he method of claim 1 wherein:

during the deriving step, suspicious activity is tracked (Desai, paragraph [0054]); and

subsequent to the deriving step, the suspicious activity is reported to a system administrator (Desai, paragraphs [0076]-[0077]).

In claim 12, Desai, as modified, discloses the method of claim 1 wherein a duration of performing the deriving step is determined by statistical means (Desai, paragraph [0062]).

In claims 13 and 19, Desai, as modified, discloses the method and computer-readable medium of claims 1 and 16, respectively, further comprising, subsequent to the deriving step, as operational step in which commands that are accessing the computer code are compared against the set of acceptable commands (Harkins, col. 2, lines 56-58).

In claim 14, Desai, as modified, discloses the method of claim 13 wherein a command that is accessing the computer code during the operational step that does not match a command in the set of acceptable commands is flagged as suspicious (Desai, paragraph [0054]).

In claim 15, Desai, as modified, discloses the method of claim 14 wherein, when a command is flagged as suspicious, at least one of the following is performed:

an alert is sent to a system administrator (Desai, paragraphs [0076]-[0077]);

the command is not allowed to access the computer code;

the command is allowed to access the computer code, but the access is limited;

the command is augmented;

a sender of the command is investigated.

In claim 20, Desai discloses apparatus for training a computer code intrusion detection system in real time (paragraphs [0035], [0043]), but fails to disclose: a training module adapted for observing, in real time, commands that are accessing the

computer code, and for deriving from said commands, in real time, a set of acceptable commands; coupled to the set of acceptable commands, a comparison module for comparing commands that access the computer code during an operational phase with commands in the set of acceptable commands. Harkins discloses observing, in real time, commands that are accessing the computer code (col. 4, lines 13-17), and for deriving from said commands, in real time, a set of acceptable commands (col. 5, lines 41-49 – execution profiles contain frequently selected commands, thus they are similar to set of acceptable commands); coupled to the set of acceptable commands, a comparison module for comparing commands that access the computer code during an operational phase with commands in the set of acceptable commands (col. 2, lines 56-58).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system with Harkins' real time audit method that observe and derive acceptable commands, and compare commands accessing the computer to effectively examine programs during execution in real time. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system with real time auditing because it provides a quick, comprehensive analysis of a program's execution and also allows identification and resolution of any problems (Harkins, col. 2, lines 10-23).

4. Claims 7 and 18 rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and Harkins and further in view of Pandit et al., US 2003/0154402.

In claims 7 and 18, Desai and Harkins disclose the method and computer-readable medium of claims 5 and 17, respectively, but fail to disclose the categories comprise canonicalized commands; and each category is a command stripped of literal field data. Pandit discloses the categories comprise canonicalized commands (paragraph [0037] – placeholders placed in templates); and each category is a command stripped of literal field data (paragraph [0037] – data values can be entered in place of placeholders).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Desai's intrusion detection system and Harkins' real time audit method with Pandit's system of storing events utilizing canonicalized commands to serve as placeholders for events. It is for this reason that one of ordinary skill in the art would have been motivated to provide Desai's intrusion detection system and Harkins' real time audit method with canonicalized commands because it helps automate the process of creating a database.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-3, 6-12 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 10-27 of copending Application No. 10/632,857. Although the conflicting claims are not identical, they are not patentably distinct from each other because both the present application and the '857 application relate to systems and methods for performing real-time auditing of program commands relating to malicious code in databases. They both disclose categories of data, removal of literal field data, flagging suspicious commands that are being audited in real time, and use of a training phase to monitor code. The only difference is that in the present application it is claimed that acceptable commands are placed in categories as opposed to the '857 use of retrieval vectors or retrieval commands. However, this difference would have been obvious to a person of ordinary skill in the art at the time the invention was made since both are aimed at merely organizing acceptable commands that are differentiated from malicious commands.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Baker, US 6,775,657; Campbell et al., US 6,839,850; Gupta et

al., US 2006/0117386; Kohler et al., US 2004/0250134; Raikar et al., US 2004/0260945; Norton et al., US 2004/0205360; Scheidell, US 2004/0098623; Beavers, US 2003/0221123; Bruton et al., US 2003/0145226.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER